UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/518,481	12/20/2004	Motonobu Tonomura	XA-10241	4916

181 7590 03/05/2008

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
YOUSEFI, SHAHROUZ	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
03/05/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@milesstockbridge.com
sstiles@milesstockbridge.com

Office Action Summary	Application No.	Applicant(s)	
	10/518,481	TONOMURA ET AL.	
	Examiner	Art Unit	
	SHAHROUZ YOUSEFI	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/20/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: on page 10, line 19, it recited "transmission path 130" should instead be --transmission path 13--.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Macy et al. (US 2003/0212727 A1) in view of Mastrovito (WO 91/20028).

With respect to claims 1 and 2, Macy et al. teaches that first and second registers (201 and 202) (registers 210 and registers 214, see fig. 2) in which parameters having a predetermined bit length are set, respectively; a third register (203) in which data to be encrypted is set (integer registers 202and instruction pointer registers 206, see fig. 2); a matrix element computation part (30) for generating matrix elements from the values set in said first and second registers (multiplication of a generator matrix by a matrix composed of input packets, par. [0077], page 6); a matrix element register (51) for holding the matrix elements generated by said matrix element computation part (As illustrated with reference to FIG. 6, corresponding byte values (302 and 304) within the registers (310 and 320) are simultaneously multiplied modulo and an irreducible

polynomial (not shown) contained in register iMM 330 to form a plurality of byte result values 306 (306-1, . . . 306-16), which are stored in a result data storage device 340, par. [0080], page7); and said matrix element computation part selectively generates matrix elements for error detection and matrix elements for encryption by changing the parameters to be set in said first and second registers (encryption and error control coding utilizing modular multiplication are within the embodiments of the present invention, par. [0128]), Macy et al. don't teach inner product calculation. But Mastrovito teaches an inner product calculation part (40) for executing inner product calculation between the matrix elements held by said matrix element register and the data set in said third register (product C can be obtained by computing the m inner products Z, page 4, line 10), and said inner product calculation part selectively performs error control code generation and data encryption by altering the matrix elements to be held in said matrix element register (Unit 2 computes the m inner products $c_j = z._j.B_j j=0,1..,m-1$, page 5, line 9).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Macy et al. to include the inner product calculation of Mastrovito to compute product in Galois fields and implement error detection, error correction and data encryption, and also allowing a product-sum calculation device to be shared.

With respect to claim 3, Macy et al. teaches that said matrix element computation part generates matrix elements for error detection, and said inner product calculation part generates an error detection code corresponding to the data set in said third

register (perform encrypting and error control using a general-purpose processor, par. [0053]).

With respect to claim 4, Macy et al. teaches that coefficient data (g') of a polynomial g(x) of degree n of Galois field is set, except for a coefficient of the highest degree n, to said first and second registers, and said inner product calculation part outputs a CRC code corresponding to a modulus (mod) of the polynomial g(x) for the data set in said third register (Referring again to $GF(2^8)$ finite field operations, such finite field operations can be described in terms of more familiar polynomial operations, par. [0072]).

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Macy et al. (US 2003/0212727 A1) in view of Mastrovito (WO 91/20028) and further in view of Brandstrom (US 4,322,577).

With respect to claim 5, Brandstrom teaches that said matrix element computation part generates matrix elements for encryption, and said inner product calculation part outputs an encryption code of the data set in said third register (These elements are used to generate a plaintext matrix which is multiplied from the right in a first matrix multiplier by a first key matrix belonging to a prescribed matrix group over the Galois-field and being generated by means of a first encryption key which is applied to a first matrix generator, the output of which is multiplied from the left in a second matrix multiplier by a second key matrix belonging to the same matrix group and being generated by means of a second encryption key which is applied to a second matrix generator, col. 3, lines 44-54).

With respect to claim 6, Brandstrom teaches that a first memory for storing coefficient data of an irreducible polynomial g(x) of degree n of Galois field and encrypti on key data; a control part (70) for reading out from said memory the coefficient data and the encryption key data in a form divided into a plurality of data blocks and setting them in said first and second registers, respectively, and a second memory for storing elements values of a plurality of partial matrices, wherein elements of a plurality of partial of matrix of n.times.n are generated by said matrix element computation part (30), and under the control of said control part, the elements of partial matrix generated by said matrix element computation part are stored in said second memory, the elements of partial matrix are selectively loaded from said second memory to said matrix element register (51), and said inner product calculation part repeats the inner product calculation between the data set in said third register and the elements of a plurality of partial matrices, thereby to output said encryption code (As an example, we get 6.multidot.7=D. By storing in a ROM or PROM memory in the multiplication table of matrices intended to be used in a cryptosystem according to the present invention, the product of matrices is easily obtained by a table-look-up routine, col. 5, lines 37-42).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Macy et al. (US 2003/0212727 A1) in view of Mastrovito (WO 91/20028) and further in view of Brandstrom (US 4,322,577) and further more in view of Toyo Communication Equipment Co., Ltd. (JP 2001-56640).

With respect to claim 7, means (52 and 53) for performing exclusive OR operation between the results of inner product calculation generated by said inner

product calculation part and pre-computed elements held as intermediate results of the calculation, and holding the results of exclusive OR operation as new intermediate results of the calculation (The 1st exclusive-OR means which performs EXCLUSIVE OR operation about each combination of the result of this EXCLUSIVE OR operation that performs EXCLUSIVE OR operation fulfills said conditions, and the result of an operation of said AND means EXCLUSIVE OR operation is performed, and it has the 2nd exclusive-OR means which obtains each bit of said vector D, and is constituted by each bit of the result of an operation of said AND means to fulfill said conditions, or said 1st exclusive-OR means and said vector C, paragraph [0010] and EXCLUSIVE OR element 202, the sum-of-products arithmetic unit 100 realizes the sum-of-products operation on Galois field GF (2m) according to said conditional expression 1, par. [0017]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is (571) 270-3558. The examiner can normally be reached on Monday-Thursday 9:00-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. Y./
Shahrouz Yousefi
Examiner
02/22/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132